CompTIA Advanced Security Practitioner (CASP+)

ID CASP+ **Preis** auf Anfrage **Dauer** 5 Tage

Voraussetzungen

Sie müssen zehn Jahre Erfahrung in der IT Administration aufweisen, davon mindestens fünf Jahre technischer Sicherheitserfahrung. Ein CASP+ Training folgt in der Regel auf ein CompTIA Security+ Training oder einen gleichwertigen Kurs, dies ist aber keine zwingende Voraussetzung.

Kursziele

In diesem Kurs erlangen Sie fortgeschrittene Fähigkeiten, die Sie benötigen, um eine Sicherheitslösung in einem komplexen Geschäftsumfeld zu entwerfen und zu erstellen.

Ihr Trainer, ein Experte in diesem Gebiet, wird Sie mit technischem Wissen und Fähigkeiten ausstatten, die erforderlich sind, um Sicherheitslösungen in komplexen Umgebungen zu konzipieren, zu entwickeln, zu integrieren und zu implementieren und so ein widerstandsfähiges Unternehmen zu unterstützen.

Sie werden ausserdem folgende Themen behandeln:

- Betriebssicherheit, einschliesslich Operations und Architecture Konzepten, Techniken und Anforderungen
- Risikoanalyse und Cyber-Abwehr-Antizipation
- Sicherheit von undefinedmobilen Geräten mit kleinem Formfaktor
- Software Schwachstellen
- Integration von Cloud- und Visualisierungstechnologien in einer sicheren Unternehmensstruktur
- Kryptographische Techniken wie Blockchain-Cryptocurrency und Mobile Device Encryption

Kursinhalt

1.0 Risk Management (19% of exam)

- Summarise business and industry influences and associated security risks.
- Compare and contrast security, privacy policies and procedures based on organisational requirements.
- Given a scenario, execute risk mitigation strategies and controls.
- Analyse risk metric scenarios to secure the enterprise.

2.0 Enterprise Security Architecture (25% of exam)

- Analyse a scenario and integrate network and security components, concepts and architectures to meet security requirements.
- Analyse a scenario to integrate security controls for host devices to meet security requirements.
- Analyse a scenario to integrate security controls for mobile and small form factor devices to meet security requirements.
- Given software vulnerability scenarios, select appropriate security controls

3.0 Enterprise Security Operations (20% of exam)

- Given a scenario, conduct a security assessment using the appropriate methods.
- Analyse a scenario or output, and select the appropriate tool for a security assessment.
- Given a scenario, implement incident response and recovery procedures

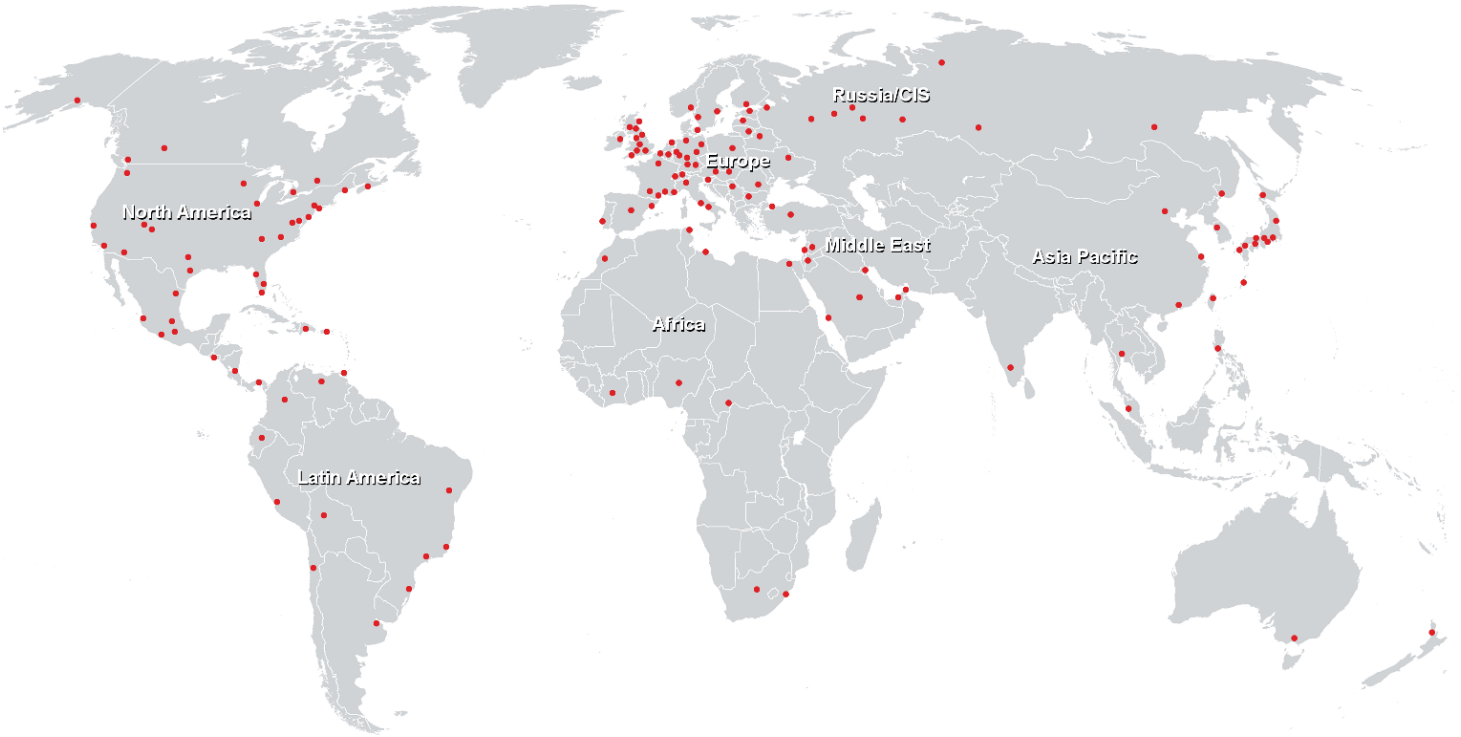
4.0 Technical Integration of Enterprise Security (23% of exam)

- Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.
- Given a scenario, integrate cloud and virtualisation technologies into a secure enterprise architecture.
- Given a scenario, integrate and troubleshoot advanced authentication and authorisation technologies to support enterprise security objectives.
- Given a scenario, implement cryptographic techniques.
- Given a scenario, select the appropriate control to secure communications and collaboration solutions.

5.0 Research, Development and Collaboration (13% of exam)

- Given a scenario, apply research methods to determine industry trends and their impact to the enterprise
- Given a scenario, implement security activities across the technology life cycle.
- Explain the importance of interaction across diverse business units to achieve security goals.

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch